

[WP-020]

## Whitepaper: Misconfigured Email: Is Your IT Department Breaking the Law?

A Discussion about the Legal Risks of Improperly Configured Email Servers

**Version 050524**

May 2005

Author: Todd Glassey, [tglassey@unixworks.com](mailto:tglassey@unixworks.com)

Author: Bob Radvanovsky, [rsradvan@unixworks.com](mailto:rsradvan@unixworks.com)

*(A special thanks goes to those listed for being my “sounding board” on this project.)*

Copyright © 2005 Todd Glassey and Bob Radvanovsky. All rights reserved.



Whitepaper [WP-020]: Misconfigured Email Services...Illegal?

Copyright © 2005 Todd Glassey and Bob Radvanovsky. All rights reserved.

“knowledge squared is information shared.”

web:[www.unixworks.com](http://www.unixworks.com) / email:[info@unixworks.com](mailto:info@unixworks.com).

Page 1

## Legal Disclaimer

---

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material. *The authors are not lawyers, and this should not be construed as legal advice, but rather as an analysis of everyday operating procedure and common sense.*

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for the purpose of discussing a possible, and/or proposed IT security issue, and is not dependent upon any specified infrastructure, architectural condition or its issue(s).

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.

## Is your email configuration causing you to be a reverse-spammer?

---

Today's spam epidemic has been made worse by a new class of spam, one that of misdirected reply messages. These "replies to spam messages" constitute (possibly) as much as 40% (if not more) of the total spam sent daily; this volume of unnecessary email traffic causes not only real damage to the Internet and corporate email gateways, but involves the initial recipients of spam in the directed re-broadcasting of that spam to a third and unrelated party.

## Electronic mail systems

---

Electronic mail (or "email") today is the core of most business communications, within, and across the enterprise, and throughout the Internet. Paperless transactions through email and other mediums now dominate how global transactions are completed. With the shift towards a paperless economics come some newly emerging requirements. These set of requirements are driven by law and human processes rather than technological invention and response.



As such, these emerging requirements are become more noticeable visible, and as such, begin to carry and hold significance within and throughout the business communities. These requirements, although treated casually and with little or no regard of their ramifications, are being viewed more highly from a legal context. Thus, their impact upon those businesses that would other disregard them, are beginning to take notice, esp. with news media coverage being so omnipresent.

*These issues pertain and are related to – **spam** – which are unsolicited electronic mail messages sent to unknowing and/or unwilling recipients, without approval or prior knowledge.*

## **“I’ll have spam, spam, sausage, egg and spam”...**

---

Unsolicited Commercial Email (UCE) with forged headers (the most virulent form of “*spam*”) now consumes much of the Internet’s capacity and it is because of that, that the intentional creation of more spam through improperly configured, mismanaged, or improperly maintained mail servers (technically referred to as “*Mail Transport Agents*” or “*MTA’s*”) is potentially becoming both criminal and civil in nature. Because of Spam email’s capability to halt commerce, there is legislation at state and federal levels within the United States that has been designed to make criminal the creation, distribution and propagation of “*spam*” with forged headers..

Other countries are now following suit in attacking these “forged header” spammers who specialize in their hit-and-run spamming. Countries such as Great Britain, France, and Germany, are developing similar or more rigorous legislation. The following link provides a listing of SPAM acts globally: <http://spamlinks.net/legal.htm#country>

One such piece of legislation that stands out is the CAN-SPAM Act of 2003<sup>1</sup>:

The Controlling the Assault of Non-Solicited Pornography and Marketing Act requires unsolicited commercial electronic mail messages to be labeled (though not by a standard method) and to include opt-out instructions and the sender’s physical address. It prohibits the use of deceptive Subject: lines and false email header information in such messages. The FTC is authorized (but not required) to establish a “do-not-email” registry. State laws that require labels on unsolicited commercial email messages or prohibit such messages entirely are pre-empted, although provisions merely addressing falsity and deception would remain in place. The CAN-SPAM Act took effect on January 1, 2004.

The CAN-SPAM Act of 2003 was introduced by Senators Conrad R. Burns (R-MT) and Ron Wyden (D-OR) in April, 2003, with minor changes from the previous year’s version, S.630 (2002). Two other bills (S.1231 and S.1293) were subsequently merged into it. The final version was approved by the U.S. Senate in November, 2003 and by the House of Representatives in December, 2003, and was signed into law by President Bush on December 16, 2003.

---

<sup>1</sup> <http://www.ftc.gov/bcp/online/pubs/buspubs/canspam.htm>.



## **Improperly configuring the email gateway may create a whole new class of spam...**

---

The law is rather specific in its requirements, and it is the authors' assertion that the improperly configured MTA that automatically or through the actions of a filter enables the sending or forwarding of email to the RETURN-PATH ADDRESS (simply called the "RETURN ADDRESS") could potentially be a new and criminal act of spam is not properly resolved and the return address proven to be the source of the spam. That is to say, if the email address originating the spam is not the same as that of the return path, then the spam cannot be forwarded on or a failure message sent to that person or entity names in the return path. This is obviously true in headers of email that are forged because the RETURN-PATH contains the forged name of the purported sender. The problem is that not doing the proper amount of diligence and verifying the RETURN-ADDRESSEE is the actual sender, then the email gateway becomes the willing co-conspirator after the fact with the original spammer to spam the Individual named in the RETURN-ADDRESS. Thus, an improperly configured set of email filters in the email gateway or ant-virus systems could be breaking the law by creating a second, and independent act of spam, where the gateway is re-broadcasting the spam to the party named in the return address.

Recently, under California statute, California Law §17529.1(c) states that "commercial e-mail advertisement" means "any electronic mail message initiated for the purpose of advertising or promoting the lease, sale, rental, gift offer, or other disposition of any property, goods, services, or extension of credit"<sup>2</sup>.

In this case, the relaying of a file attachment may be interpreted to constitute the property (if you will) that is attached to the incoming email message. In all cases, the intentional relaying of viral or malicious software attachments constitutes a second and separately prosecutable even under all the Computer Fraud and Abuse Act of 1996, and most all spam laws within this country, whether this is done as part of a bounced or rejected email message practice, or otherwise as part of a pre-processing methodology of the email message performed by a automated process, such as content filter, virus filter, spam and consistency checker, etc., or appliance.

## **Anti-virus/anti-spam services and the "Level of Care" concept**

---

Anti-virus services represent an instance where some level of care was exerted above generic practices to eliminate either spam, malicious software (virus software, Trojan Horses, worms, etc.) or both – within attachments. This creates a concept called the "expected level of care", and as such, is representative that if spam and/or malicious email messages were sent via the email server operator's gateway, and processed the email header completely and properly, it would know that the sending address was not valid, thus returning the email message to the stated return email address.

---

<sup>2</sup> [http://www.market4profit.net/california\\_anti\\_spam\\_law.html](http://www.market4profit.net/california_anti_spam_law.html).



Note that this is *supposedly* the returning email address of the originating sender, but since the email message (and its header) has been forged, the intent is for the mail server to reject the email and label it as “spam”, thus returning an error message, with the spam content within the email message, to its target – which, indirectly, is being delivered by the unknowing and unwilling recipient’s mailbox *by their own email server!*

From the “level of care” concept, any efforts of protecting the recipient from spam must perform due diligence thoroughly and completely; otherwise, even with partial completeness of whatever remediation efforts to remove the spam from the SMTP stream to the intended (or in this case, indirectly intended) recipient, could potentially be held responsible as being the the new source for the bouncing spam and NOT the original spamming party. This potentially poses serious legal risk towards, and provides some teeth with the meaning of “*due diligence*”.

Reiterating again, the unknowing and unwilling recipient does NOT know that he/she is about to receive an email. With an improperly configured email server, spam email is received by the email server and rejected back to the supposedly originating party, which it turns out, is our unknowing and unwilling recipient. In doing so with the rejection of the email message, now the email server is relaying spammed email messages to their intended parties – without having to know of any elaborate or sophisticated methods of camouflaging or masquerade their email message headers. They simply forge the RETURN-PATH ADDRESS with the intended recipient that is to receive the spam, and then utilizing the email server as the delivery mechanism!

The problem with the header processing is the expense in system cycles and overhead. Most email servers are (most often than not) already over-taxed, and adding the necessity of resolving each and every email message with its corresponding “*Domain Name Services*” (or “*DNS*”) to verify that the sending email header matches the sender’s email domain address would significantly increase the amount of system (and perhaps, network) overhead. The point is that systems administrators disable these extra validation features to save bandwidth and processing time. The problem with this scenario, is that ANY processing of the email message headers, including (especially) the anti-virus and anti-spam stages of the verification process, then obligates the owner of the email server to also conduct DNS resolution verification checks, such that the email server will know whether or not if the address being returned email was forged or not. Overall, the recommended course of action is simply to NOT return any bounced or rejected email correspondence to an address that cannot be resolved and that is identical to the SENDER’s DOMAIN ADDRESS.

Many systems and email administrators have taken an age-old stance of configuring their email systems to reject certain incoming emails, and to bounce them back to the sending, originating name(s) within the RETURN PATH or SENDER fields in the email message header. The problem is that in the case of fraudulently sent spam email, those headers are forged and so the act of resending these emails is actually a second violation of the CAN-SPAM act because of the “standard of care” and “willful negligence” standards under the law.



What does this represent to an email administrator from a legal perspective? Only the courts can truly say what is or is not a legal violation of the law. Additionally, they have not yet ruled on these matters; however, what is obvious is that doing anything -- viral filtration, user name lookup, alias processing, or anything really to the email within its inbound path obligates one to “do everything reasonably possible”, and to validate the email sender address, either when the email was initially received or as part of a “BOUNCING EMAIL” rule in the email server itself. Not only is the statement about that the overhead is too costly simply not an excuse for the commission of a criminal act, but the reasoning behind those concerns were for an earlier Internet, not today’s robust and reliable network. So when spam is bounced without validating the headers the effects are clear.

About 30 years ago, when email was traversing the ARPANet for the first time, there was no need to authenticate the users,. While full header filtration and its validation could have easily been performed, the lack of the robustness of the “Net”, along with limited networking bandwidth, as well as limited access to DNS services, meant that this processing was very cumbersome and time consuming, so unilaterally systems and mail administrators made a decision to simply “just turn off the header validation”.

What this means is that generally when someone sends an email message to someone that is considered “spam”, the email header generally will have bad or easily parsed data in it, outlaying that it is clearly “*spam*”. Most of the techniques usually involve some form of email header forging, but can get rather sophisticated if a multi-level marketing (called “MLM”) company has abilities to eradicate all legitimate forms of information within the email header, thus completely and utterly forging the entire email message, from header to subject line, to the entire content of the message itself.

For instance, within the email header (shown on the subsequent page) – this piece of email came from network IP address **218.254.74.39**, with the name ***caremailsmtp1.prontomail.com***, but in fact, the reverse DNS for this IP address resolves to ***cm218-254-74-39.hkcable.com.hk***, which is either a dial-up or leased address belonging to an ISP in Hong Kong, China.

Leased lines can be as simple as dial-up connections, but now include broadband cable, DSL, and ISDN – all of which allow for temporary assignment of a networked address during the duration of the connection. Once the connection has been severed, and re-established, it is often times a totally different IP address.



This poses a serious problem for network security analysts in traceability issues, esp. when dealing with “spam” (the email header is outlined in RED and YELLOW colors; the YELLOW is the actual email IP address, RED is the forged email IP address)

```
Received: from caremailsmtp1.prontomail.com (cm218-254-74-39.hkcable.com.hk[218.254.74.39](untrusted sender))
      by worldnet.att.net (mtiwmxc11) with SMTP
      id <2005052412565201100j54gge>; Tue, 24 May 2005 12:56:58 +0000
X-Originating-IP: [218.254.74.39]
Reply-To: "Holly Smith" <kmkujyvucashette.com>
From: "Holly Smith" <kmkujyvucashette.com>
To: <gramgramp@att.net>
Subject: Miracle protein kills all viruses
Date: Tue, 24 May 2005 08:55:59 -0400
Content-Type: multipart/alternative;
      boundary="--09-4[5]-7222-3[3]-041[3]"
-----09-4[5]-7222-3[3]-041[3]
```

For more information about how email message headers are formed, visit the Wikipedia definition on “SMTP Header”, which may be found here:

[http://en.wikipedia.org/wiki/Simple\\_Mail\\_Transfer\\_Protocol](http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol).

Other protocol documents that relate to email message exchange may be found here:

<http://www.ietf.org/rfc/rfc2821.txt>

<http://www.ietf.org/rfc/rfc2822.txt>

Further investigation of the IP address reveals the following information:

```
inetnum:      218.252.0.0 - 218.255.255.255
netname:      HKCABLE-HK
descr:        HK Cable TV Ltd
descr:        Cable Multi-Media Services
country:      HK
admin-c:      AD23-AP
tech-c:       AD23-AP
mnt-by:       APNIC-HM
mnt-lower:    MAINT-HK-ICABLE
remarks:      include previous allocations
changed:      hm-changed@apnic.net 20030922
status:       ALLOCATED PORTABLE
source:       APNIC
person:       administrator dns
address:      12/F., Cable TV Tower,
address:      9 Hoi Shing Road,
address:      Tsuen Wan,
address:      N.T.,
address:      HK
country:      HK
phone:        +852-2112-7516
fax-no:       +852-2112-7977
e-mail:       dnsadmin@cms.hkcable.com
nic-hdl:      AD23-AP
mnt-by:       MAINT-HK-ICABLE
changed:      dnsadmin@cms.hkcable.com 20000811
source:       APNIC
```



This was through the web site controlled by the Asian-Pacific Network Information Center (APNIC) (<http://www.apnic.net/apnic-bin/whois.pl>).

That means with one check, an analyst or administrator would know that it is 99.999% positive that they would be unable to contact this person once they sent the mail. Any amount of research also will show ProntoMail to be a US company in Folsom, CA.

Domain name registration for the domain name “**prantomail.com**” reveals that the whois registration is inaccurate (lacking phone numbers for contact) but still resolvable to a U.S. based domain name and street address.

```
Registrant Contact:
  CP Software Group, Inc.
  Domain Administrator (domain_admin@mailcentro.com)
  Fax:
  715 Sutter Street
  Folsom, CA 95630
  US
```

It is most likely that this company has nothing to do with the Hong Kong address sending the forged email, the spammer used to send the spam in the first place meaning that their name was forged by someone using a service in another jurisdiction to spam U.S. recipients with this email address.

What that means is that the individual receiving this email could, if they bothered to expend the effort, determine with very little overhead today, that this is in fact an instance of a forged email spam message, and that it's original senders, who are not the people listed in the RETURN ADDRESS or SENDER PATH fields, are not where it came from.

## Conclusion

---

Legally speaking – with negligence standards in the current state they are today -- makes bouncing any suspected spammed email message a legal risk and possibly opens the entity or person receiving the spam itself to prosecution under the same CAN-SPAM act's provisions for the negligent re-distribution of fraudulently addressed mail.



## About the Authors

---

Todd Glassey is author of Wiley Interscience *“Techbriefs: PKI”* (edited by Tom Austin), and is an active participant in the IT forensics and auditing discussion forums and its communities. Todd’s experiences have included designing a secured time stamping protocol and mechanism, time and space digital key generator, location authentication protocol, and has been noodling around with UNIX since 1981. Todd is an experienced network security design architect and engineer and former EGG ‘black ops’ specialist, holding numerous certifications: *Certified Information Security Manager* (CISM) from ISACA; *Certified Information Forensics Investigator* (CIFI) from IISFA.

Bob Radvanovsky is the author of *“Fundamental Concepts in Critical Infrastructure Preparedness”* (to be available in Summer 2005), and is an active participant in the information and networking security technology forums and discussion groups. Bob’s experiences have included Department of Defense risk assessments, penetration testing and analysis, IT auditing and forensics, and user-community educational forums. Bob’s background stems from his initial days with AT&T UNIX System III back in 1978, has several degrees in business and computer science studies, and holds several certifications: *Certified Information Security Manager* (CISM) from ISACA; *Certified Information Forensics Investigator* (CIFI) from IISFA; *Certified Infrastructure Preparedness Specialist* (CIPS) from the Office of Infrastructure Preparedness.



## Appendix A

---

The following information (shown below and on subsequent pages) is an example of an indirectly intended recipient from spam:

---

This is the Postfix program at host atlrel8.hp.com.

I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to <postmaster>

If you do so, please include this problem report. You can delete your own text from the attached returned message.

The Postfix program

```
<Alain.Robert@cup.hp.com>: host smtp.cup.hp.com[15.1.28.250] said: 550
  <Alain.Robert@cup.hp.com>: Recipient address rejected: User unknown in
  local recipient table (in reply to RCPT TO command)

<Dannis_Yang@cup.hp.com>: host smtp.cup.hp.com[15.1.28.250] said: 550
  <Dannis_Yang@cup.hp.com>: Recipient address rejected: User unknown in local
  recipient table (in reply to RCPT TO command)

<Kevin.Welton@cup.hp.com>: host smtp.cup.hp.com[15.1.28.250] said: 550
  <Kevin.Welton@cup.hp.com>: Recipient address rejected: User unknown in
  local recipient table (in reply to RCPT TO command)

<Matthias.Riese@cup.hp.com>: host smtp.cup.hp.com[15.1.28.250] said: 550
  <Matthias.Riese@cup.hp.com>: Recipient address rejected: User unknown in
  local recipient table (in reply to RCPT TO command)

<Trevor@cup.hp.com>: host smtp.cup.hp.com[15.1.28.250] said: 550
  <Trevor@cup.hp.com>: Recipient address rejected: User unknown in local
  recipient table (in reply to RCPT TO command)

<andrew.johnson@cup.hp.com>: host smtp.cup.hp.com[15.1.28.250] said: 550
  <andrew.johnson@cup.hp.com>: Recipient address rejected: User unknown in
  local recipient table (in reply to RCPT TO command)

<andysc@cup.hp.com>: host smtp.cup.hp.com[15.1.28.250] said: 550
  <andysc@cup.hp.com>: Recipient address rejected: User unknown in local
  recipient table (in reply to RCPT TO command)

<antoni.wolski@cup.hp.com>: host smtp.cup.hp.com[15.1.28.250] said: 550
  <antoni.wolski@cup.hp.com>: Recipient address rejected: User unknown in
  local recipient table (in reply to RCPT TO command)

<bbryan@cup.hp.com>: host smtp.cup.hp.com[15.1.28.250] said: 550
  <bbryan@cup.hp.com>: Recipient address rejected: User unknown in local
  recipient table (in reply to RCPT TO command)

<brucel@cup.hp.com>: host smtp.cup.hp.com[15.1.28.250] said: 550
  <brucel@cup.hp.com>: Recipient address rejected: User unknown in local
  recipient table (in reply to RCPT TO command)

<d.finkler@cup.hp.com>: host smtp.cup.hp.com[15.1.28.250] said: 550
  <d.finkler@cup.hp.com>: Recipient address rejected: User unknown in local
```



recipient table (in reply to RCPT TO command)

<[dth@cup.hp.com](mailto:dth@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.250] said: 550 <[dth@cup.hp.com](mailto:dth@cup.hp.com)>:  
Recipient address rejected: User unknown in local recipient table (in reply  
to RCPT TO command)

<[edlund@cup.hp.com](mailto:edlund@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.250] said: 550  
<[edlund@cup.hp.com](mailto:edlund@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[franco@cup.hp.com](mailto:franco@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.250] said: 550  
<[franco@cup.hp.com](mailto:franco@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[fscwritte@cup.hp.com](mailto:fscwritte@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.250] said: 550  
<[fscwritte@cup.hp.com](mailto:fscwritte@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[fy@cup.hp.com](mailto:fy@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.250] said: 550 <[fy@cup.hp.com](mailto:fy@cup.hp.com)>:  
Recipient address rejected: User unknown in local recipient table (in reply  
to RCPT TO command)

<[graham@cup.hp.com](mailto:graham@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.250] said: 550  
<[graham@cup.hp.com](mailto:graham@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[howard.yin@cup.hp.com](mailto:howard.yin@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.250] said: 550  
<[howard.yin@cup.hp.com](mailto:howard.yin@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[hwolin@cup.hp.com](mailto:hwolin@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.250] said: 550  
<[hwolin@cup.hp.com](mailto:hwolin@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[ivan@cup.hp.com](mailto:ivan@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.250] said: 550  
<[ivan@cup.hp.com](mailto:ivan@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[j.h.hermans@cup.hp.com](mailto:j.h.hermans@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[j.h.hermans@cup.hp.com](mailto:j.h.hermans@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[jamin@cup.hp.com](mailto:jamin@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[jamin@cup.hp.com](mailto:jamin@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[kabe@cup.hp.com](mailto:kabe@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[kabe@cup.hp.com](mailto:kabe@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[keith.thompson@cup.hp.com](mailto:keith.thompson@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[keith.thompson@cup.hp.com](mailto:keith.thompson@cup.hp.com)>: Recipient address rejected: User unknown in  
local recipient table (in reply to RCPT TO command)

<[king@cup.hp.com](mailto:king@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[king@cup.hp.com](mailto:king@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[koliver@cup.hp.com](mailto:koliver@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[koliver@cup.hp.com](mailto:koliver@cup.hp.com)>: Recipient address rejected: User unknown in local  
recipient table (in reply to RCPT TO command)

<[meganwoods@cup.hp.com](mailto:meganwoods@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550



<[meganwoods@cup.hp.com](mailto:meganwoods@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[miyahara@cup.hp.com](mailto:miyahara@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[miyahara@cup.hp.com](mailto:miyahara@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[mmester@cup.hp.com](mailto:mmester@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[mmester@cup.hp.com](mailto:mmester@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[mww@cup.hp.com](mailto:mww@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550 <[mww@cup.hp.com](mailto:mww@cup.hp.com)>:  
Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[mzunke@cup.hp.com](mailto:mzunke@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[mzunke@cup.hp.com](mailto:mzunke@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[nick@cup.hp.com](mailto:nick@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[nick@cup.hp.com](mailto:nick@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[pritham@cup.hp.com](mailto:pritham@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[pritham@cup.hp.com](mailto:pritham@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[ps@cup.hp.com](mailto:ps@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550 <[ps@cup.hp.com](mailto:ps@cup.hp.com)>:  
Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[r.kay@cup.hp.com](mailto:r.kay@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[r.kay@cup.hp.com](mailto:r.kay@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[richard\\_maxwell@cup.hp.com](mailto:richard_maxwell@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[richard\\_maxwell@cup.hp.com](mailto:richard_maxwell@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[rthrashe@cup.hp.com](mailto:rthrashe@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[rthrashe@cup.hp.com](mailto:rthrashe@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[sdun@cup.hp.com](mailto:sdun@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[sdun@cup.hp.com](mailto:sdun@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[sheila\\_devins@cup.hp.com](mailto:sheila_devins@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[sheila\\_devins@cup.hp.com](mailto:sheila_devins@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)

<[simon.j.parker@cup.hp.com](mailto:simon.j.parker@cup.hp.com)>: host smtp.cup.hp.com[15.1.28.240] said: 550  
<[simon.j.parker@cup.hp.com](mailto:simon.j.parker@cup.hp.com)>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command)



## Appendix B

---

The following information (shown below and on subsequent pages) is an example of an indirectly intended recipient from spam:

---

This is the Postfix program at host futurnet.es.

I'm sorry to have to inform you that the message returned below could not be delivered to one or more destinations.

For further assistance, please send mail to <postmaster>

If you do so, please include this problem report. You can delete your own text from the message returned below.

The Postfix program

<[abilbrey@futurnet.es](mailto:abilbrey@futurnet.es)>: unknown user: "abilbrey"  
<[brad.strand@futurnet.es](mailto:brad.strand@futurnet.es)>: unknown user: "brad.strand"  
<[cflynn@futurnet.es](mailto:cflynn@futurnet.es)>: unknown user: "cflynn"  
<[crock@futurnet.es](mailto:crock@futurnet.es)>: unknown user: "crock"  
<[Daisy\\_Tam@futurnet.es](mailto:Daisy_Tam@futurnet.es)>: unknown user: "daisy\_tam"  
<[engd@futurnet.es](mailto:engd@futurnet.es)>: unknown user: "engd"  
<[jrj@futurnet.es](mailto:jrj@futurnet.es)>: unknown user: "jrj"  
<[Malcolm\\_Graham@futurnet.es](mailto:Malcolm_Graham@futurnet.es)>: unknown user: "malcolm\_graham"  
<[mk@futurnet.es](mailto:mk@futurnet.es)>: unknown user: "mk"  
<[pbannister@futurnet.es](mailto:pbannister@futurnet.es)>: unknown user: "pbannister"  
<[rapson@futurnet.es](mailto:rapson@futurnet.es)>: unknown user: "rapson"  
<[rmosh@futurnet.es](mailto:rmosh@futurnet.es)>: unknown user: "rmosh"  
<[romeo@futurnet.es](mailto:romeo@futurnet.es)>: unknown user: "romeo"  
<[scottk@futurnet.es](mailto:scottk@futurnet.es)>: unknown user: "scottk"  
<[shafriri@futurnet.es](mailto:shafriri@futurnet.es)>: unknown user: "shafriri"  
<[tobin.j.schuster@futurnet.es](mailto:tobin.j.schuster@futurnet.es)>: unknown user: "tobin.j.schuster"  
<[tschleu@futurnet.es](mailto:tschleu@futurnet.es)>: unknown user: "tschleu"  
<[cdk@futurnet.es](mailto:cdk@futurnet.es)>: unknown user: "cdk"  
<[alan.b.butt@futurnet.es](mailto:alan.b.butt@futurnet.es)>: unknown user: "alan.b.butt"  
<[chrisb@futurnet.es](mailto:chrisb@futurnet.es)>: unknown user: "chrisb"  
<[mindlace@futurnet.es](mailto:mindlace@futurnet.es)>: unknown user: "mindlace"



<[eugen@futurnet.es](mailto:eugen@futurnet.es)>: unknown user: "eugen"  
<[John.McKernan@futurnet.es](mailto:John.McKernan@futurnet.es)>: unknown user: "john.mckernan"  
<[chrisp@futurnet.es](mailto:chrisp@futurnet.es)>: unknown user: "chrisp"  
<[John.Wood@futurnet.es](mailto:John.Wood@futurnet.es)>: unknown user: "john.wood"  
<[iang@futurnet.es](mailto:iang@futurnet.es)>: unknown user: "iang"  
<[vbrauner@futurnet.es](mailto:vbrauner@futurnet.es)>: unknown user: "vbrauner"  
<[kern@futurnet.es](mailto:kern@futurnet.es)>: unknown user: "kern"  
<[mattj@futurnet.es](mailto:mattj@futurnet.es)>: unknown user: "mattj"  
<[Fred\\_Yao@futurnet.es](mailto:Fred_Yao@futurnet.es)>: unknown user: "fred\_yao"  
<[djones@futurnet.es](mailto:djones@futurnet.es)>: unknown user: "djones"  
<[amanda-core@futurnet.es](mailto:amanda-core@futurnet.es)>: unknown user: "amanda-core"  
<[Denis.Girault@futurnet.es](mailto:Denis.Girault@futurnet.es)>: unknown user: "denis.girault"  
<[CurtisB@futurnet.es](mailto:CurtisB@futurnet.es)>: unknown user: "curtisb"  
<[cfc@futurnet.es](mailto:cfc@futurnet.es)>: unknown user: "cfc"  
<[msamson@futurnet.es](mailto:msamson@futurnet.es)>: unknown user: "msamson"  
<[maffeis@futurnet.es](mailto:maffeis@futurnet.es)>: unknown user: "maffeis"  
<[bae@futurnet.es](mailto:bae@futurnet.es)>: unknown user: "bae"  
<[curt.ellmann@futurnet.es](mailto:curt.ellmann@futurnet.es)>: unknown user: "curt.ellmann"  
<[rohan@futurnet.es](mailto:rohan@futurnet.es)>: unknown user: "rohan"  
<[mlewan0@futurnet.es](mailto:mlewan0@futurnet.es)>: unknown user: "mlewan0"  
<[ravi.tavakley@futurnet.es](mailto:ravi.tavakley@futurnet.es)>: unknown user: "ravi.tavakley"  
<[pg@futurnet.es](mailto:pg@futurnet.es)>: unknown user: "pg"  
<[portmaster@futurnet.es](mailto:portmaster@futurnet.es)>: unknown user: "portmaster"  
<[jgrimbart@futurnet.es](mailto:jgrimbart@futurnet.es)>: unknown user: "jgrimbart"  
<[reedc@futurnet.es](mailto:reedc@futurnet.es)>: unknown user: "reedc"  
<[anoop@futurnet.es](mailto:anoop@futurnet.es)>: unknown user: "anoop"  
<[jeffryd@futurnet.es](mailto:jeffryd@futurnet.es)>: unknown user: "jeffryd"  
<[saar@futurnet.es](mailto:saar@futurnet.es)>: unknown user: "saar"  
<[itsao@futurnet.es](mailto:itsao@futurnet.es)>: unknown user: "itsao"



## Appendix C

---

The following information (shown below and on subsequent pages) is an example of an indirectly intended recipient from spam. In both cases, the original email contained German sentences:

---

Lese selbst:  
<http://brandenburg.rz.fhtw-berlin.de/poetschke.html>

*Indeed, this may be part of a worm, Trojan Horse, virus or other malicious software (called “malware”) that may have compromised a system, and is now broadcasting to everyone it can send email messages to.*

## Appendix D

---

The following information (shown below and on subsequent pages) is an example of an indirectly intended recipient from spam. This is a sample of a rejected email message.

---

This is an automatically generated Delivery Status Notification.

Delivery to the following recipients failed.

samplec@protransintl.com  
sahdalas@protransintl.com

